

REMARKS

I. Status of the Claims:

Reconsideration and allowance of the claims pending in the application are requested.

Claims 1-31 are pending in the application.

Claim 31 is rejected under 35 USC 112, first paragraph, as failing to comply with the written description requirement.

Claims 24 and 31 are rejected under 35 USC 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 1-31 are rejected under 35 USC 101 because the claimed invention is directed to non-statutory subject matter.

Response to the Rejections under 35 USC 112, First and Second Paragraphs:

Paragraphs 1 - 4

The Examiner's comments are noted.

Paragraph 5:

Applicants traverse the rejection under 35 USC 112, First Paragraph that claim 31 does not comply with the written description requirement based on there is no support in the specification for the feature "generating a computational task by a first server for a certain amount of intense computation in a specified period of time as a POW to accomplish a separate, useful and verifiable correct computation;" as follows:

Applicants direct the Examiner's attention to the specification at page 3, line 13, continuing to page 4, line 2 where it is stated:

"As shown in FIGS. 1A and 1B, the architecture comprises entities 1, 2 and 3 through n (all of which may be servers). Although entity 1 is illustrated in FIGS. 1A and 1B as being distinct from entity 2, in an alternate embodiment, entities 1 and 2 may be the same entity. To begin, with reference to FIG. 1A, entity 1 has a computational task to perform. In furtherance of

that task, (A) entity 1 instructs entity 2 to perform some computational work related to the task. Entity 2 will then out-source the work related to the task to each of entities 3 through n. Outsourcing may be accomplished by dividing the work into components and assigning each entity 3 through n a different component. As shown in FIG. 1B, as (B) each entity 3 through n completes its component of work, each entity will respond with its reply. Each of the replies is a POW (referred to herein as "POW₁"). Entity 2 then compiles (compiles) the replies into a response and transmits the response to entity 1. This response is also a POW (referred to herein as "POW₂"). Finally, (C) entity 1 verifies the response."

Applicants submit the terms "generating a computational task by a first server" are described by the above underlined portion of the specification, identified as (A).

Applicants further submit the terms "for a certain amount of intense computation in a specified period of time as a POW" are described by the underlined portion of the specification, identified as (B).

Applicants further submit the terms "to accomplish a separate, useful and verifiable correct computation" are identified by the underlined portion of the specification, identified as (C), taken in conjunction the underlined portion of the specification at page 2, lines 14-17 identified as (D), where it is stated, "Whereas the traditional bread pudding recipe recycles stale bread, a bread pudding protocol recycles the "stale" computations in a POW to perform a separate and useful operation,(D) while also maintaining privacy in the operation."

Applicants submit that a worker skilled in the art, particularly the computational art, has sufficient disclosure from the above cited specification pages to implement the claimed feature.

The rejection of claim 31 under 35 USC 112, First Paragraph has been overcome by the indicated disclosures in the specification. Withdrawal of the rejection of claim 31 under 35 USC 112, First Paragraph is requested.

Paragraph 6:

Applicants traverse the rejection of claims 24 and 31 under 35 USC 112, Second Paragraph based on the phrases "certain amount", "intense" and "useful" as indefinite terms.

First, with regard to the phrases “certain amount” and “intense”, applicants direct the Examiner’s attention to the specification at page 5, line 12 continuing to page 6, line 4, which state, as follows:

“The aim of a POW is to enable P to demonstrate that she has performed a certain amount of computation within the time interval $[-t_s, t_c]$. Let poly denote any polynomial in a given variable. (We use the informal notation poly(x) to denote a polynomial in the variable x, and $o(1 / \text{poly}(x))$ to denote a quantity that is asymptotically smaller than the inverse of any polynomial in x.) Finally, let l be a security parameter. Finally, let us assume that the prover is permitted to perform an arbitrarily large amount of computation prior to the protocol execution. Thus, in fact, our definitions assume that the prover may perform computation over the time interval $[-\infty, t_c]$. We characterize the hardness of a POW using the following two definitions, where probabilities are over the coin flips of both parties, and computational steps and memory resources are as measured in any suitable model. Definition 1 provides the notion of a lower bound on POW hardness, while Definition 2 provides that of an upper bound.

Definition 1: We say that a proof of work POW is (w, p)-hard if the following is true. Suppose prover P with memory resources bounded by m performs an average, over all coin flips by P and V, of at most w steps of computation in the time interval $[t_s, t_c]$. Then the verifier V accepts with probability at most $p + o\left(\frac{m}{\text{poly}(l)}\right)$, where l is a security parameter.

Definition 2: We say that a proof of work POW is (w, p, m)-feasible if there exists a prover P with memory resources bounded by m such that with an average of w steps of computation in the time interval $[t_s, t_c]$, the prover can cause the verifier V to accept with probability at least p. This leads to the following definition.

Applicants submit the Definitions 1 and 2 define the phrases “certain amount” and “intense” by the number of flips of at most w steps of computation in the time interval t_s, t_c for a verifier to accept a POW with at least a probability p.

A worker skilled in the art, particularly one skilled in the computational art, has sufficient information from the cited specification pages to implement the claimed feature in which the phrases “certain amount” and ”intense” are used.

Second, with regard to the phrase “useful”, applicants direct the Examiner’s attention to the specification at page 1, line 13-16 which states, as follows:

“Although not defined as such or treated formally in the literature, POWs have served as the basis for a number of data security applications, including, benchmarking, server access metering, construction of digital time capsules, and protection against spamming and other denial-of-service attacks.”(E)

Applicants submit the above specification portion, identified as (E) describes separate and useful applications of POWs. A worker skilled in the art, particularly the computational arts would recognize the usefulness of the claimed subject matter.

The rejection of claims 24 and 31 under 35 USC 112, Second Paragraph has been overcome by the indicated disclosures in the specification. Withdrawal of the rejection of claims 24 and 31 under 35 USC 112, Second Paragraph is requested.

Response to the Rejection under 35 USC 101:

Paragraph 7:

Applicants understand the Examiner to contend that claims 1-31 describe non-statutory subject matter in the form of a computational effort performing a Proof of Work.

Applicants disagree with the Examiner’s contention, as follows:

First, the MPEP at 2106(IV)(B) (1) states “a claim describes non-statutory subject matter if it consist solely of mathematical operations without some claimed practical application (i.e., executing a “mathematical algorithm”).

In the present instance, claims 1-31 describe a process for distributing a computational task among several entities to perform portions of the task in terms of POWs, which when compiled perform a useful task in a number different applications, particularly security applications, minting coins. Further the process makes available the POWs for reuse in other applications. Clearly, claims 1-31 describe practical applications of the claimed subject matter and describe statutory subject matter, not non-statutory subject matter based on the definition of the above cited MPEP reference.

Second, The MPEP at 2106(IV)(B)(1a) states “Office personnel should determine whether the computer program is being claimed as part of an otherwise statutory manufacture or

machine. In such a case, the claim remains statutory irrespective of the fact that a computer program is included in the claim. The same result occurs when a computer program is used in a computerized process where the computer executes the instructions set forth in the computer a statutory process program. Only when the claimed invention taken as a whole is directed to a mere program listing, i.e., to only its description or expression, is it descriptive material per se and hence non-statutory.”

Applicants submit claims 1-31 describe a statutory process, which incorporates into the process a computerized computation. Based on the above cited MPEP reference. the claims remain statutory irrespective of the fact that a computerized process is included in the claim, particularly when the claimed subject matter has practical applications.

Third, MPEP 2106(IV)(B(1b) states “The presence of the claimed nonfunctional descriptive material is not necessarily determinative of non-statutory subject matter. For example, a computer that recognizes a particular grouping of musical notes read from memory and upon recognizing that particular sequence, causes another defined series of notes to be played, defines a functional interrelationship among that data and the computing processes performed when utilizing that data, and as such is statutory because it implements a statutory process.”

In the present instance, claims 1-31 describe grouping or compiling of POWs, which serve as a basis for a number of security applications. Claims 1-31 describe statutory subject matter, even assuming the POWs describe non-statutory subject matter, based on the above cited MPEP reference.

Summarizing, the rejection of claims 1-31 under 35 USC 101 as non-statutory subject matter is in error based on (a) the claims have a practical application and are statutory; (b) the alleged non-statutory subject matter, i.e. computational task is part of an otherwise statutory process, and the claims remain statutory, and (c) the claims have support in the MPEP as statutory subject matter. Withdrawal of the rejection of claims 1 -31 under 35 USC 101 is requested.

CONCLUSION

Applicants have support in the specification for the terms and phrases in the claimed subject matter. The rejection of claim 31 under 35 USC 112 First Paragraph and the rejection of claims 24 and 31 under 35 USC 112, Second Paragraph have been overcome. Further, applicants have demonstrated claims 1-31 are not in conflict with 35 USC 101, and the rejection under 35 USC 101 has been overcome. Claims 1-31 have been deemed allowable subject matter. Having overcome all rejections of claims 1-31, applicants request entry of the amendment, allowance of claims 1-31, and passage to issue of the case.

AUTHORIZATION

The Commissioner is hereby authorized to charge any additional fees which may be required for consideration of this Amendment to Deposit Account No. 13-4500, Order No. JAKOBSSON 23-5 (3037-4196). A DUPLICATE OF THIS DOCUMENT IS ATTACHED.

In the event that an extension of time is required, or which may be required in addition to that requested in a petition for an extension of time, the Commissioner is requested to grant a petition for that extension of time which is required to make this response timely and is hereby authorized to charge any fee for such an extension of time or credit any overpayment for an extension of time to Deposit Account No. 13-4500, Order No. JAKOBSSON 23-5 (3037-4196). A DUPLICATE OF THIS DOCUMENT IS ATTACHED.

Respectfully submitted,
MORGAN & FINNEGAN, L.L.P.

Dated: December 5, 2006

By: Joseph C. Redmond, Jr.
Joseph C. Redmond, Jr.
Reg. No. 18,753
Telephone: (202) 857-7887
Facsimile: (202) 857-7929

CORRESPONDENCE ADDRESS:

Morgan & Finnegan L.L.P.
3 World Financial Center
New York New York